REMARKS

Minor amendments have been made to the specification. Specifically, on page 1, the status of one of the cited copending applications has been updated, and on page 12, a typographical error has been corrected.

Claims 1, 3, 5 to13, 15 to 25, 27 to 30, 32, and 34 to 44 are pending in the application. By this amendment, claims 1, 3, 5 to 13, 15 to 25, 27 to 30, 32 and 34 to 38 have been amended, claims 2, 4, 14, 26, 31 and 33 have been canceled, and new claims 39 to 44 have been added.

Claims 1 to 13, 25 to 30, and 33 to 35 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,961,849 to Davis et al. This rejection is believed to be moot in view of the amendments made to the independent claims 1 and 25, these claims now being limited to a method of protecting a check and a check, respectively.

Claims 14 to 24, 31, 32, and 36 to 38 were rejected under 35 U.S.C. §103(a) as being unpatentable over the patent to Davis et al. in view of U.S. Patent No. 7,181,430 to Buchanan. In making the rejection, the Examiner acknowledges that Davis et al. does not teach a check with a unique identifier X which is check data comprising a bank ID number, an account ID number and a check number and relies on Buchanan et al. for a teaching of a system for processing checks. This rejection is respectfully traversed for the reason that the combination of Davis et al. and Buchanan et al. fails to show, suggest or otherwise teach the claimed invention.

According to the claimed invention there is provided a method for protecting a check, which will be transformed into a value bearing instrument after adding additional markings to the check, from fraudulent alteration of the markings (claims 1, 3, 5 to13, and 15 to 24), a check protecting against fraudulent alteration of markings added to the check to transform the check into a value bearing instrument (claims 25, 27 to 30, 32, and 34 to 38), and an apparatus for protecting a check, which will be transformed into a value bearing instrument after adding additional markings to the check, from fraudulent alteration of the markings (new claims 30 to 44). The method and the apparatus operate to process

the check which is characterized by "having printed thereon a unique identifier X, the unique identifier including a bank ID, an account ID number and a check number, the check further having critical fields k, k=1,2,3..., the critical fields including a date field, a payee field, amount fields, a payer's field, and an endorser's field, and each critical field k, k=1,2,3..., being covered a large number of lines of fine print comprising encrypted versions the unique identifier X printed on the document, $Sign_{k0}(X)$, where $Sign_{k0}(X)$ is a cryptographic function or family thereof which is known only to an institution which issues the document, $Sign_{k0}(X)$ being used to authenticate the document" (claim 25). No such check is even remotely suggested by the combination of Davis et al. and Buchanan et al. More particularly, the check is characterized by having "each critical field k of the check, in addition to being covered by encrypted versions of X, $Sign_{k0}(X)$, . . . [being] covered with another encrypted version of X, $Sign_k(X)$, where $Sign_k(X)$ is another cryptographic function or family thereof different from the cryptographic function $Sign_{k,0}(X)$ which is known to a larger number of authorized institutions for performing an initial authentication of the document" (claim 27; see also claim 34 which is dependent on claim 32), and having "each critical field k of the check, in addition to being covered by encrypted versions of X, $Sign_{k,0}(X)$ and $Sign_k(X)$, . . . [being] covered with a third encrypted version of X, $Sec_k(X)$ is another cryptographic function or family thereof different from the cryptographic functions $Sign_{k,0}(X)$ and $Sign_k(X)$ which is known to a small group within the institution which issues the document for performing final authentication of the document" (claim 28; see also claim 35 which is dependent on claim 34). To further enhance the protection of the check against fraud, the "cryptographic functions $Sign_k$, $Sign_{k,0}$ and Sec_k, are indexed by a number corresponding to the field k, so that each line comprises different encryptions of X such that each cryptographic function $Sign_k(X)$, $Sign_{k,0}(X)$, $Sec_k(X)$ is a family of different cryptographic functions" (claim 29).

The "act of adding markings to the check to transform the check into a value bearing instrument obscures some of the encryptions, the families of different cryptographic functions preventing cryptographic functions which have been obscured at different places from being used to reconstitute the full

cryptographic function" (claim 30). Note that the invention contemplates that the very act of writing the date, payee's name, amount of the check and signing the check will obscure some of the encryptions. See also claim 32 which is dependent on claim 25.

The "encrypted function $Sign_k(X)$ is communicated to banks and other authorized institutions involved in depositing checks and the encrypted function $Sign_k(X)$ allows the payee's bank to perform a first authentication of the check" (claim 36), "key $Sign_{k,0}$ remains the exclusive property of the issuing bank and the encrypted function $Sign_{k,0}(X)$ is used exclusively by the issuing bank and branches involved in the clearing of checks" (claim 37), and "secret key Sec_k is exclusively known to the issuing bank and the encrypted function $Sec_k(X)$ is used by the issuing bank as a final instrument to verify the check" (claim 38).

According to the claimed method, this check is produced by first "generating encryptions of a unique identifier X of the document, the unique identifier X being check data including a bank ID, an account ID number and a check number printed on the check, the encryptions being $Sign_{k,0}(X)$, where $Sign_{k,0}(X)$ is a cryptographic function or family thereof which is known only to an institution which issues the check, $Sign_{k,0}(X)$ being used to authenticate the check" and then "covering each critical field k, k=1,2,3..., of the check where markings are to be added with a large number of lines of fine print, the lines of fine print comprising the cryptographic function $Sign_k$, the critical fields k including a date field, a payee field, amount fields, a payer's signature field, and an endorser's field" (claim 1). In addition, "each critical field k of the document, in addition to being covered by the encrypted version of X, $Sign_{k,0}(X)$, is covered with another encrypted version of X, $Sign_k(X)$, where $Sign_k(X)$ is another cryptographic function or family thereof different from the cryptographic function $Sign_{k,0}(X)$ which is known to a larger number of authorized institutions for performing an initial authentication of the check" (claim 3). Further, "each critical field k of the check, in addition to being covered by encrypted versions of X, $Sign_k(X)$ and $Sign_{k,0}(X)$, is covered with a third encrypted version of X, $Sec_k(X)$, where $Sec_k(X)$ is another cryptographic function or family thereof different from the cryptographic functions $Sign_{k,0}(X)$ and $Sign_k(X)$ which is known to a small group

within the institution which issues the check for performing final authentication of the check" (claim 5). Security is further enhanced by "indexing the cryptographic functions $Sign_k$, $Sign_{k,0}$ and Sec_k, by a number corresponding to the field k, so that each line comprises different encryptions of X such that each cryptographic function $Sign_k(X)$, $Sign_{k,0}(X)$ and $Sec_k(X)$ is a family of different cryptographic functions" (claim 6), and "the families of cryptographic functions $Sign_k$, $Sign_{k,0}$ and Sec_k prevent cryptographic functions which have been obscured at different places by marks added to the check from being used to reconstitute the full cryptographic function" (claim 7).

The manner in which the check is authenticated involves "generating a digitized version of the check in at least selected locations where markings are added to transform the check into a value bearing instrument; extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, $Sign_k(X)$, which is known to a large number of authorized institutions; and comparing a decrypted version of $Sign_k(X)$ to the unique identifier X as an initial authentication of the check" (claim 10), "extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, $Sign_{k,0}(X)$, which is known only to an institution that issues the check; and comparing a decrypted version of $Sign_{k,0}(X)$ to the unique identifier X as a further authentication of the check" (claim 11), and "extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, $Sec_k(X)$, which is known to a small group within the institution that issues the check; and comparing a decrypted version of $Sec_k(X)$ to the unique identifier X as a final authentication of the check" (claim 12). The manner in which the encryptions $Sign(X)$ and $Sign_k(X)$ are computed and the key $Sec_k(X)$ is chosen is set out in claims 15, 16 and 17, respectively.

A particular advantage of the method according to the claimed invention is that the check can be deposited from home or other location remote from the bank by scanning and transmitting, as set out in claims 8, 9 and 18. As previously noted, the act of adding writing to the check obscures portions of the lines of fine print bearing the encryptions (claim 13). Claims 19 to 22 parallel claims 10 to 12, while claims 23 and 24 further limit claim 19.

Turning now to the primary reference to Davis et al., this reference discloses a method for selectively encrypting one or more elements of a document using style sheet processing using, for example, an Extensible Stylesheet Language, or "XSL", processor that creates a selectively encrypted document, such as an Extensible Markup Language, or "XML", document carrying key-distribution material such that by using an augmented document processor, such as an augmented XML processing engine, an agent can recover only the information elements for which it is authorized. The Document Type Definition (DTD) or schema associated with a document is modified, such that the DTD or schema specifies a reference to stored security policy to be applied to document elements. Each document element may specify a different security policy, such that different elements of a single document can be encrypted differently (and, some elements may remain unencrypted). The key distribution material enables a document to be encrypted for decryption by an audience that is unknown at the time of the document creation, and enables access to the distinct elements of a single encrypted document to be controlled for multiple users and/or groups of users. In this manner, group collaboration is improved by giving more people easier access to information for which they are authorized.

Notice first of all that Davis et al. describe a system for selectively encrypting different elements of a document with different levels of security such that various persons or groups of persons are limited in the level of access they are permitted to certain of the different elements of the document. In contrast, the claimed invention is intended to prevent fraud by protecting the entire document, i.e., the check. The Davis et al. system and method is most applicable to group collaboration wherein in different members of the group are given different levels of authorization to access certain elements of the document.

The Examiner is correct that Davis et al. has nothing to do with checks, but the addition of the Buchanan et al. reference does not cure this deficiency. Buchanan et al. discloses a system which captures and securely transmits check images, deposit information and other information from remote locations for the purpose of having those checks credited to the depositing individual's or organization's bank account(s) and having the check images (and/or physical

checks) entered into the bank check clearing channels for ultimate delivery to the maker bank for payment out of the maker's account. Thus, Buchanan et al. is more relevant to the claimed invention than Davis et al., but Buchanan et al. do not employ the type of check specifically recited in claims 25, 27 to 30, 32, and 34 to 38 and the method of using that type of check recited in claims 1, 3, 5 to 13, and 15 to 24. More specifically, there is no suggestion in Buchanan et al. of a check wherein critical fields (i.e., date field, payee field, amount fields, payer's field, and endorser's field) are covered by a large number of lines of fine print comprising encrypted versions of a unique identifier (i.e., bank ID, account ID, and check number), portions of which are obscured by the act of filling out the critical fields by the maker and the endorser. Moreover, the combination of Buchanan et al. with Davis et al. would not result in a suggestion or teaching of such a check and the method of using that type of check.

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 1, 3, 5 to 13, and 15 to 25, 27 to 30, 32, and 34 to 44 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

A provisional petition is hereby made for any extension of time necessary for the continued pendency during the life of this application. Please charge any fees for such provisional petition and any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 50-2041.

Respectfully submitted,

C. Lamont Whitham
Reg. No. 22,424

Whitham, Curtis, Christofferson & Cook, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190
Tel. (703) 787-9400
Fax. (703) 787-7557
Customer No.: 30743